Formulating and Reasoning About Security Policies: Final Report

Joseph Y. Halpern

Grant No: AFOSR F49620-02-1-0101
PI: Joseph Y. Halpern
Institution: Cornell University, Ithaca, NY 14853

Objectives

The goal of this project was to investigate the use of first-order logic for expressing security policies and reasoning about authorization, and to apply to logic for use with digital library and other applications.

Status

Accomplishments

As discussed above, semantics were given to XrML and ODRL. Our work on XrML, which also involved finding problems with various XrML constructs, had a significant influence on the 2004 release of XrML. The work on ODRL resulted in Vicky Weissman (who was supported by this grant) being asked to serve on the ODRL working group. The Lithium work has caught the attention of a group at NRL, who are now planning to implement it for their work on policies. The papers covering this work, "Using first-order logic to reason about policies", "A formal foundation for XrML", "Towards a policy language for humans and computers", and "A formal foundation for ODRL", appeared in leading conferences (see below for details).

Digital Rights Management is a major topic of interest both in industry and the military. This work—with its focus on precise semantics for policies, understanding the expressive power of languages actually used, and making digital rights languages more usable by nonexperts—thus has the potential for having a major impact. It has already attracted a great deal of attention.

REPORT DOCUMENTATION PAGE	*Form Approved* *OMB No. 074-0188*

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing this collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188), Washington, DC 20503

1. AGENCY USE ONLY (Leave blank)	**2. REPORT DATE** **March 31, 2005**	**3. REPORT TYPE AND DATES COVERED** Final Jan 2002 – Dec 2004

4. TITLE AND SUBTITLE Formulating and Reasoning About Security Policies	**5. FUNDING NUMBERS** F49620-02-1-0101
6. AUTHOR(S) Halpern, Joseph Y.	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Cornell University 120 Day Hall Ithaca, NY 14853	**8. PERFORMING ORGANIZATION REPORT NUMBER** OSP# 40792
9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES) Air Force Office of Scientific Research 4015 Wilson Blvd., Room 713 Arlington, VA 22203-1954	**10. SPONSORING / MONITORING AGENCY REPORT NUMBER**

11. SUPPLEMENTARY NOTES

12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for Public Release; distribution is Unlimited	**12b. DISTRIBUTION CODE**

13. ABSTRACT ***(Maximum 200 Words)***

The goal of this project was to investigate the use of first-order logic for expressing security policies and reasoning about authorization, and to apply to logic for use with digital library and other applications. Major progress was made in (1) giving semantics to currently-used digital rights languages (XrML and ODRL), (2) understanding the limitations in expressive power of current languages, (3) identifying a fragment of first-order logic that is appropriate for reasoning about security (Lithium), and (4) providing an interface for expressing policies that nonexperts can use (Rosetta). Digital Rights Management is a major topic of interest both in industry and the military. This work---with its focus on precise semantics for policies, understanding the expressive power of languages actually used, and making digital rights languages more usable by nonexperts---thus has the potential for having a major impact.

14. SUBJECT TERMS Digital rights management, security policies, authorization	**15. NUMBER OF PAGES** 7
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT U	**18. SECURITY CLASSIFICATION OF THIS PAGE** U	**19. SECURITY CLASSIFICATION OF ABSTRACT** U	**20. LIMITATION OF ABSTRACT** UU

Personnel Supported

Victoria Weissman (graduate student), Joseph Halpern (PI).

Publications

Articles in Journals

1. J. Y. Halpern, Characterizing the common prior assumption, *Journal of Economic Theory* **106**:2, 2002, pp. 316–355.
2. J. Y. Halpern and R. Pucella, A logic for reasoning about upper probabilities, *Journal of AI Research* **17**, pp. 57-81, 2002.
3. P. Grünwald and J. Y. Halpern, Updating probabilities, *Journal of AI Research* **19**, 2003, pp. 243–278 (with P. Grünwald).
4. J. Y. Halpern, A computer scientist looks at game theory, *Games and Economic Behavior* **45**:1, 2003, pp. 114–132.
5. J. Y. Halpern and R. van der Meyden, A logical reconstruction of SPKI, *Journal of Computer Security* **11**:4, 2003, pp. 581–614.
6. J. Y. Halpern and R. Pucella, On the relationship between strand spaces and multi-agent systems, *ACM Transactions on Information and System Security* **6**:1, 2003, pp. 43–70.
7. J. Y. Halpern and L. Li, A minimum-energy path-preserving topology-control algorithm, *IEEE Transactions on Wireless Communications* **3**:3, 2004, pp. 910–921.
8. J. Y. Halpern, R. van der Meyden, and M. Y. Vardi, Complete axiomatizations for reasoning about knowledge and time, *SIAM Journal on Computing* **33**:2, 2004, pp. 674–703.
9. J. Y. Halpern and D. Koller, Representation dependence in probabilistic inference, *Journal of AI Research* **21**, pp. 319-356, 2004.
10. J. Y. Halpern and R. Shore, Reasoning about common knowledge with infinitely many agents, *Information and Computation* **191**:1, 2004, pp. 1–40.
11. J. Y. Halpern and Y. Moses, Using counterfactuals in knowledge-based programming, *Distributed Computing* **17**:2, 2004, pp. 91–106.
12. H. Chockler and J.Y. Halpern, Responsibility and blame: A structural-model approach, *Journal of AI Research* **22**, 2004, pp. 93–115.

13. F. Chu and J. Y. Halpern, Great expectations. Part II: Generalized expected utility as a universal decision rule, *Artificial Intelligence* **159**:1,2, 2004, pp. 207–230.

14. L. Li, J. Y. Halpern, P. Bahl, Y.-M. Wang, and R. Wattenhofer, A cone-based distributed topology-control algorithm for wireless multi-hop networks, *IEEE/ACM Transactions on Networking*, **13**:1, 2005, pp. 147-159.

15. J. Y. Halpern and A. Ricciardi, A knowledge-theoretic analysis of uniform distributed coordination and failure detectors, to appear, *Distributed Computing.*

16. J. Y. Halpern and J. Pearl, Causes and explanations: A structural-model approach—Part I: Causes, to appear, *British Journal for the Philosophy of Science.*

17. J. Y. Halpern and J. Pearl, Causes and explanations: A structural-model approach—Part II: Explanation, to appear, *British Journal for the Philosophy of Science.*

18. J. Y. Halpern and K. O'Neill, Anonymity and information hiding in multiagent systems, to appear, *Journal of Computer Security.*

Articles in Refereed Conference Proceedings

1. Z. Haas, J. Y. Halpern, and L. Li, Gossip-based ad hoc routing, *Proceedings of Infocom*, 2002, pp. 1707–1716.

2. F. Chu, J. Gehrke, and J. Y. Halpern, Least expected cost query optimization: What can we expect? *Proceedings of the 21st ACM Symposium on Principles of Database Systems*, 2002, pp. 293-302

3. J. Y. Halpern and K. O'Neill, Secrecy in multi-agent systems, *Proceedings of the 15th IEEE Computer Security Foundations Workshop*, 2002, pp. 32-46.

4. P. Grünwald and J. Y. Halpern, Updating probabilities, *Proceedings of the Eighteenth Conference on Uncertainty in AI*, 2002, pp. 187–196.

5. J. Y. Halpern and R. Pucella, Reasoning about Expectation, *Proceedings of the Eighteenth Conference on Uncertainty in AI*, 2002, pp. 207–215.

6. J. Y. Halpern and R. Pucella, Modeling adversaries in a logic for security protocol analysis, *Formal Aspects of Security: First International Conference (FASec 2002)*, Lecture Notes in Computer Science, vol. 2629, Springer, 2003, pp. 115–132.

7. R. Pucella and V. Weissman, A logic for reasoning about digital rights, *Proceedings of the 15th IEEE Computer Security Foundations Workshop*, 2002, pp. 282–294.

8. J. Y. Halpern and V. Weissman, Using first-order logic to reason about policies, *Proceedings of the 16th IEEE Computer Security Foundations Workshop*, 2003, pp. 187–201.

9. J. Y. Halpern and K. O'Neill, Anonymity and information hiding in multiagent systems, *Proceedings of the 16th IEEE Computer Security Foundations Workshop*, 2003 pp. 75-88.

10. F. Chu and J. Y. Halpern, Great expectations. Part I: On the customizability of generalized expected utility, *Proceedings of the 18th International Joint Conference on Artificial Intelligence (IJCAI 2003)*, 2003, pp. 291–296.

11. F. Chu and J. Y. Halpern, Great expectations. Part II: Generalized expected utility as a universal decision rule, *Proceedings of the 18th International Joint Conference on Artificial Intelligence (IJCAI 2003)*, 2003, pp. 297–302.

12. H. Chockler and J. Y. Halpern, Responsibility and blame: A atructural-model approach, *Proceedings of the 18th International Joint Conference on Artificial Intelligence (IJCAI 2003)*, 2003, pp. 147–153.

13. J. Y. Halpern and R. Pucella, Probabilistic algorithmic knowledge, *Proceedings of the Ninth Conference on Theoretical Aspects of Rationality and Knowledge*, 2003, pp. 118–130.

14. J. Y. Halpern and R. Pucella, A Logic for Reasoning about Evidence, *Proceedings of the Nineteenth Conference on Uncertainty in AI*, 2003, pp. 297–304.

15. J. Y. Halpern and V. Teague, Rational secret sharing and multiparty computation, *Proceedings of 36th ACM Symposium on Theory of Computing*, 2004, pp. 623–632.

16. J. Y. Halpern, Sleeping Beauty reconsidered: Conditioning and reflection in asynchronous systems, *Ninth International Conference on Principles of Knowledge Representation and Reasoning (KR 2004)*, 2004, pp. 12-22.

17. J. Y. Halpern, Intransitivity and vagueness, *Ninth International Conference on Principles of Knowledge Representation and Reasoning (KR 2004)*, 2004, pp. 121-129.

18. J. Y. Halpen and V. Weissman, A formal foundation for XrML, *Proceedings of the 17th IEEE Computer Security Foundations Workshop*, 2004, pp. 251–263.

19. P. Grünwald and J. Y. Halpern, When ignorance is bliss, *Proceedings of the Twenthieth Conference on Uncertainty in AI*, 2004, pp. 226–234.

20. M. M. Halldórsson, J. Y. Halpern, L. Li, and V. Mirrokni, On spectrum sharing games, *Procedings of the Twenty-Third Annual ACM Symposium on Principles of Distributed Computing*, 2004, pp. 107–114.

21. K. Bhargavan, C. Fournet, A. D. Gordon, and R. Pucella, ”TulaFale: A security tool for web services”, *Formal Methods for Components and Objects (FMCO 2003)*, to appear, *Lecture Notes in Computer Science*, Springer-Verlag, 2004.

22. C. Lagoze and V. Weissman, Towards a policy language for humans and computers, to appear, *Proceedings of the 8th European Conference on Digital Libraries (ECDL'04)*, 2004.

23. R. Pucella and V. Weissman, A formal foundation for ODRL, *Proceedings of the Workshop on Issues in the Theory of Security (WITS'04)*, 2004.

24. R. Pucella and V. Weissman, Reasoning about dynamic policies, *Proceedings of the 7th International Conference on Foundations of Software Science and Computation Structures (FOSSACS'04)*, Lecture Notes in Computer Science 2987, pp. 453-467, Springer-Verlag, 2004.

Participation/Interactions

Joseph Halpern gave the following talks:

- Causes and Explanations: A Structural-Model Approach
  - Invited Talk, Dutch Theory Day, Utrecht (March, 2002).
  - Invited Talk, Workshop on the Unusual Effectiveness of Logic in Computer Science, Saarbrucken (March, 2002).
  - Invited Talk, Utrecht University (June, 2002)
- Substantive Rationality and Backward Induction,
  - Invited Talk, Conference on Dimensions in Epistemic Logic, Roskilde, Denmark (May, 2002).
  - Stern School of Business, New York University, April, 2003.
- Using first-order logic to reason about policies
  - AFOSR Software Systems and Information Fusion Annual Workshop, Syracuse, (June, 2002).
  - Cornell Informatation Assurance Institute Workshop, Cornell University, March, 2003.
  - AFRL, Rome, New York, July, 2003.
- Updating probabilities, Eighteenth Conference on Uncertainty in AI, Edmonton, Canada (August, 2002).
- Reasoning about Expectation, Eighteenth Conference on Uncertainty in AI, Edmonton, Canada, (August, 2002).
- Reasoning about Uncertainty,

    - University of Illinois, Chicago Circle, January, 2003.
    - Invited talk, MFCSIT 2004 (Third Irish Conference on the Mathematical Foundations of Computer Science and Information Technology), Dublin, Ireland (July, 2004).

- Great expectations: on the utility of expected utility, University of Toronto, May, 2003.

- Probabilistic algorithmic knowledge, Ninth Conference on Theoretical Aspects of Rationality and Knowledge, Indianapolis, June, 2003.

- Characterizing the common prior assumption, Invited talk, XV IMGTA (15th Italian Meeting on Game Theory and Applications), Urbino, Italy, July, 2003.

- Great expectations. Part I: On the customizability of generalized expected utility, 18th International Joint Conference on Artificial Intelligence (IJCAI 2003), Acapulco, Mexico, August, 2003.

- Great expectations. Part II: Generalized expected utility as a universal decision rule, 18th International Joint Conference on Artificial Intelligence (IJCAI 2003), Acapulco, Mexico, August, 2003.

- Responsibility and blame: A atructural-model approach, 18th International Joint Conference on Artificial Intelligence (IJCAI 2003), Acapulco, Mexico, August, 2003.

- A Logic for Reasoning about Evidence, Nineteenth Conference on Uncertainty in AI, 2003, Acapulco, Mexico, August, 2003.

- Rational Secret Sharing and Multiparty Computation
    - Invited talk, Cowles Foundation Workshop on Complexity in Economic Theory, Yale University (September, 2003).
    - Invited talk, Second World Congress of Game Theory, Marseilles (July, 2004).

- A formal foundation for XrML,
    - AFOSR Software and Systems Workshop, Cornell University (May, 2004).
    - AFRL, Rome, New York (June, 2004).

- Using counterfactuals in knowledge-based programming, Invited talk, CombLog '04 (Workshop on Combination of Logics: Theory and Applications, Lisbon, Portugal (July 2004).

- Anonymity and information hiding in multiagent systems, Invited talk, First IEEE Symposium on Multi-Agent Security and Survivability, Philadelphia (August, 2004).

Victoria Weissman gave the following talks:

- A logic for reasoning about digital rights,
  - Workshop on Issues in the Theory of Security (WITS'02) Portland OR (January 2002).
  - 15th IEEE Computer Security Foundations Workshop, Keltic Lodge, Nova Scotia (June, 2002)
- Using first-order logic to reason about policies,
  - 16th Computer Security Foundations Workshop, Asilomar, California, July, 2003.
  - OSD/MURI secure mobile code workshop, Cornell, July, 2003.
- A formal foundation for XrML,
  - University of Pennsylvania, Philadelphia, March, 2004.
  - 17th Computer Security Foundations Workshop, Asilomar, California, July, 2004.

New discoveries, inventions or patent disclosures

None.

Honors/Aweards

- Chosen ACM Fellow, November, 2002.
- Fulbright Fellow, 2001-02.
- Guggenheim Fellow, 2001-02.
- Awarded 1997 Gödel Prize for outstanding paper in the area of theoretical computer science for "Knowledge and common knowledge in a distributed environment".
- Fellow of the American Association of Artificial Intelligence, 1993.